МОДЕЛЬ ЗАЩИТЫ МУЛЬТИМЕДИЙНОГО КОНТАКТ-ЦЕНТРА ОТ DDoS-АТАК НА ОСНОВЕ ПАКЕТНОГО ФИЛЬТРА В РАМКАХ ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ПОДХОДА

В.Н. Максименко, *доцент кафедры «Информационная безопасность» МТУСИ, к.т.н. vladmaks @yandex.ru*

УДК 621.391

Аннотация. Переход к цифровой экономике сделал востребованным исследование особенностей больших информационных систем и разработку новых методов проектирования, удовлетворяющих критериям качества и безопасности. В предлагаемой статье анализируется аспект безопасности и приводятся результаты моделирования защиты мультимедийного контакт-центра от DDoS-атак для инженерного проектирования с использованием объектно-ориентированного подхода, CASE-средств и визуального языка моделирования UML.

Ключевые слова: контакт-центр; информационная безопасность; доступность; целостность; конфиденциальность; диаграмма; информационная инфраструктура.

MODEL OF PROTECTION OF THE MULTIMEDIA CONTACT CENTER FROM DDoS-ATTACKS ON THE BASIS OF THE PACKET FILTER WITHIN THE FRAMEWORK OF THE OBJECT-ORIENTED APPROACH

Vladimir Maksimenko, *associate professor of the «Information security» department» MTUCI, candidate of technical sciences.*

Annotation. The transition to a digital economy has made it necessary to study the characteristics of large information systems and the development of new design methods that meet the criteria of quality and safety. The proposed article analyzes the security aspect, and presents the results of modeling the protection of a multimedia contact center from DDoS attacks for engineering design using an object-oriented approach, CASE tools and the visual modeling language UML.

Keywords: contact center; information security; availability; integrity; confidentiality; diagram; information infrastructure.

Построение цифровой экономики выдвинуло на первый план разработку больших систем, реализующих интеллектуальную обработку информационно-справочных запросов, отвечающих потребностям запрашивающего потребителя. Необходимость оперативной реакции на запросы потребителей делает актуальным использование высокоскоростных технологий обработки и передачи информации при оказании информационных услуг [1].

Методы функционального и структурного распараллеливания, применявшиеся на ранних этапах использования высокопроизводительных вычислительных систем, учитывали только особенности архитектуры и топологии сосредоточенных высокопроизводительных вычислительных систем и не учитывали возможности создания распределенных вычислительных систем [2, 3]. Объектно-ориентированный подход, не имея концептуального разрыва между структурой анализируемой системы и структурой вычислительной системы, позволяет осуществлять декомпозицию сложной задачи на верхнем уровне на небольшое число относительно независимых компонентов, географически распределенных или сосредоточенных [4], т.е. применим на ранних этапах проектирования, когда до алгоритмов и функций дело еще не дошло. Использование языка визуального моделирования UML и CASE-средств позволяет создавать модель быстрее, чем реальный прототип программы и, соответственно намного легче и быстрее доработать и изменить, если обсуждение покажет принятые решения неверными [4].

В предлагаемой статье использован объектно-ориентированный подход «от общего – к частному» применительно к моделированию системы защиты контакт-центра. На сегодняшний день услуги контакт-центра являются неотъемлемой частью любой компании, которая занимается продвижением своих товаров или услуг на потребительском рынке. В отличие от call-центров, которые обрабатывали заявки абонентов только по телефону, контакт–центры способны сопровождать и решать проблемы пользователей в виде текстовых сообщений по электронной почте, SMS, Web, текстовым чатам и т.д. Таким образом, контакт-центры превращаются в хранилища большого объема информации, интеллектуальная обработка которой позволяет выявить потребности и предпочтения потребителей в конкретной проблемной области [1]. Очевидно, что через некоторое время системы обработки запросов получат свое развитие в цепочке call-центр, контакт-центр, контекст-центр. Четкое определение понятия «контекст-центр» еще не сформулировано.

Либерализация рынка электросвязи способствовала повышению конкуренции как между отдельными видами связи, так и повышению конкуренции компаний, оказывающих однотипные услуги. Особенно остро это проявляется в среде аутсорсинговых контакт-центров. На первый план выдвинулись показатели качества оказываемых услуг, одной из составляющих которой являются показатели защиты информации контакт-центра [5].

В контакт-центре есть много ценной информации: клиентские и собственные базы данных, статистические и отчетные материалы, финансовая документация, журналы регистрации событий, происходящих в системе. Защита бизнеса включает обеспечение как организационно-экономической, так и технической безопасности [6].

В сфере технической безопасности необходимо решать следующие задачи:

- обеспечение надежности работы оборудования и программного обеспечения;
- защита от внутреннего и внешнего несанкционированного доступа;
- обеспечение перспектив технического развития.

Архитектура безопасности контакт-центра должна создавать препятствия для таких преднамеренных и непреднамеренных угроз, как уничтожение информации или других ресурсов, искажение или модификация информации, кражи, утечки, потеря информации и других ресурсов, разглашение конфиденциальной информации.

Система защиты информации контакт-центра от внешнего и внутреннего несанкционированного доступа реализуется как на административном, так и на технологическом уровне. При этом следует использовать такие механизмы защиты, как контроль доступа и аутентификация пользователей.

В погоне за прибылью, компании-конкуренты способны на многое. На поприще инфокоммуникационных технологий, нередко встречаются случаи заказных атак на сервисные платформы конкурентов, с помощью которых возможно вывести компанию из финансового равновесия. Самыми распространенным видом заказных атак на сегодняшнее время являются атаки типа DDoS.

DDoS-атака (Destributed Denial of Service) – это распределенная атака из многих источников, которая препятствует доступу легитимных пользователей к атакуемому ресурсу путем вывода его из строя или заполнения полосы пропускания атакуемого предприятия нелегитимным трафиком. Данному виду атак подвержены все компании, которые присутствуют в интернете. Сложность разработки алгоритма защиты от DDoS атак контакт-центра состоит в том, что прежде чем разрабатывать модель угроз и соответствующие методы защиты, необходимо проанализировать сетевые особенности построения контакт-центра, тем более, что структуры контакт-центров эволюционировали от систем, построенных на основе телефонных станций до систем, построенных на основе пакетной передачи данных, и выбрать наиболее перспективную структуру.

Основными типами DDoS-атак являются: массированные атаки, атаки на протокольном уровне и атаки на уровне приложений. В любом случае основная цель атаки в том, чтобы вывести из строя ресурс или же украсть конфиденциальные данные.

Таким образом, защита от атаки типа DDoS занимает одно из самых важных мест в информационной безопасности предприятия. Сегодня нельзя полагаться на добросовестную конкуренцию среди компаний и нужно быть всегда готовым к угрозам, как извне, так и снаружи.

Для того, чтобы разработать методы защиты от атак типа «отказ в обслуживании» требуется понять, как они работают, на что влияют и к каким последствиям приводят. Большинство компаний не задумывается об обеспечении защиты непосредственно во время протекания DDoS-атаки. Все средства, вложенные в обеспечение сетевой безопасности, в основном направлены на попытки предотвратить угрозу, восстановление работоспособности сети после атаки и расследование данного инцидента, что в конечном итоге не приведет ни к чему кроме расхода финансовых средств.

Таким образом, проблема обеспечения защиты от атак типа «отказ в обслуживании» будет актуальной на протяжении долгого времени, ведь с развитием информационных технологий появляются новые и новые методы реализации угроз информационной безопасности информационных систем.

Анализ предметной области

Контакт-центр представляет собой систему, взаимодействующую, с одной стороны, с телекоммуникационной инфраструктурой, через которую поступают запросы, а с другой – с определенными программными приложениями, призванными улучшить качество обработки этих запросов, такие как ERP, Help Desk и CRM. В зависимости от типа связи, соединяющего пользователя и оператора контакт-центра, запросы могут поступить в речевой форме, при использовании телефонной сети, или в речевой и в виде текстового сообщения при использовании интернет или сотовой связи (SMS или MMS). Контакт-центр призван обеспечить быстрое и вместе с тем качественное и защищенное обслуживание пользователя при высокой культуре общения в процессе оказания информационных услуг. Классификация и бизнес-модели контакт-центров рассмотрены в работах [6, 7]. Информационная модель мультимедийного КЦ представлена на рис. 1.

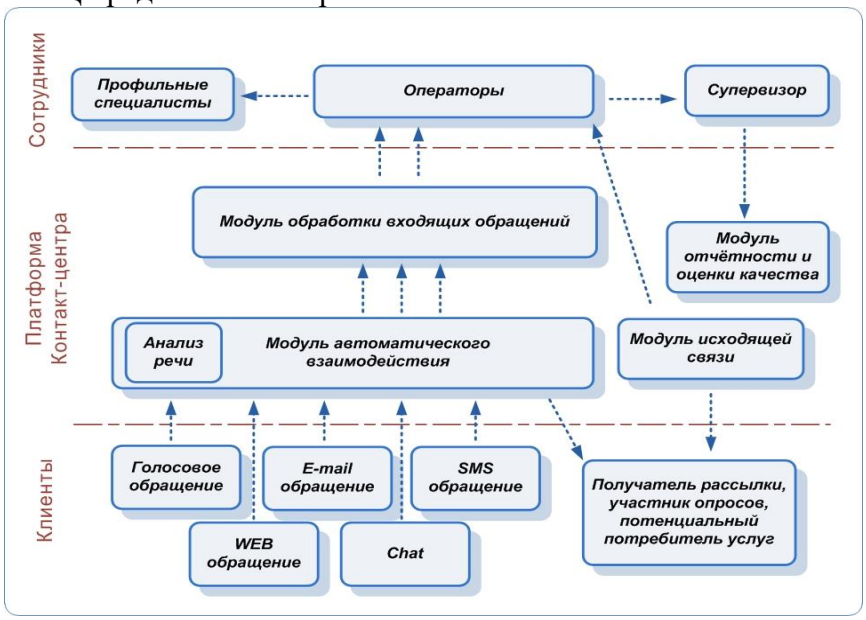

Рисунок 1

Основные функциональные возможности интегрированного КЦ напрямую зависят от типов обрабатываемых вызовов. Таким образом, дисциплины очередей и механизмы

маршрутизации в КЦ интегрированных с интернет могут быть значительно сложнее, чем в традиционных КЦ. Связано это с источниками запросов, которые имеют различные характеристики, такие как: интенсивность, время ожидания, продолжительность обслуживания, т.е. имеют разные параметры, которые определяют входящую нагрузку, на основании которой происходит распределение вызовов и организация очередей.

Во время ожидания обслуживания, клиенту доступен ряд возможностей. Традиционно при нахождении в очереди, абоненты слышат музыку, рекламные объявления и оповещения о продвижении очереди. Если клиент попал в КЦ с Web-страницы во время нахождения в очереди, он имеет возможность пользоваться сайтом, а также появляется информационное окошко, которое показывает – через какой промежуток времени будет принят вызов абонента. Если же все ресурсы КЦ заняты, то клиента оповестят о примерном времени – через которое он может перезвонить [5].

Бизнес-процессом, связанным с управлением электронными контактами, обычно занимается специально созданное подразделение КЦ, которое представляет собой:

- «горячую линию» поддержки владельцев банковских карт;
- «горячую линию» поддержки клиентов оператора сотовой мобильной связи;
- «горячую линию» поддержки заказчиков или внутреннего персонала компании – helpdesk;
- телемаркетинговый отдел, который занимается продвижением товаров и услуг компании и т.п.

Обобщающим фактором представленных подразделений КЦ является высокий объем трафика контактов, который приводит к необходимой автоматизации бизнес-процессов «контактного» подразделения для предотвращения значительных денежных потерь в связи с не оптимально настроенным рабочим процессом.

Вторым фактором является требование к обработке операторами КЦ различных типов обращений, начиная с бумажных и заканчивая электронными. Обработка всех типов обращений сотрудниками одного подразделения является экономически эффективной, так как максимально используются существующие ресурсы и упрощается процедура внедрения изменений в «контактные» бизнес-процессы, в связи с тем, что обучаются сотрудники только одного подразделения.

Третьим фактором является использование специального программного обеспечения для управления контактами: систем CRM и др. Одной из основных проблем менеджмента «контактного» подразделения является оптимизация внутренних бизнес-процессов. Без использования средств автоматизации работы КЦ положительных результатов в борьбе за прибыль добиться невозможно. Таким образом, опираясь на общие характеристики «контактных» отделов компании, такие как самостоятельность, комплексность и масштабность, а также повышенные требования к качеству работы и обслуживания, можно сформулировать требования, которые компании предъявляют к КЦ:

- многоканальная и мультимедийная обработка запросов: независимо от источника запроса (звонок или сообщение на электронную почту) запрос должен быть обработан по всем унифицированным правилам;
- глубокая интегрируемость с CRM и информационными системами, используемыми на предприятии, в информационном хранилище компании должен оставаться статический «след» контактного канала, выбранного для установления соединения;
- адаптивная система интеллектуальной маршрутизации вызова, которая будет учитывать дату, время, день недели и т.д. информации находящейся в CRM, помимо стандартных условий маршрутизации;

- использование ИБП для бесперебойной работы системы во избежание простоя сервиса, который приведет к финансовым потерям компании;
- возможность автоматизации исходящей связи с помощью возможностей систем IVR, а также исходящей связи с участием оператора КЦ;
- обеспечение дополнительных возможностей подсистем автоматизирующих обработку интернет-вызовов, таких как: возможность отслеживания истории контактов для обращений по почте (e-mail), мультичат для текстовых интернет-обращений и т.д.

За все эти требования отвечают различные компоненты сети КЦ, которые требуют соответственного обслуживания и определенного уровня сетевой и информационной безопасности.

Принципы построения телекоммуникационной инфраструктуры

Телекоммуникационная инфраструктура, используемая контакт-центрами, постоянно модернизируется, обеспечивая возможность внедрения новых услуг. Сети нового поколения NGN (от англ. Next Generation Networks – Сети Следующего Поколения) – мультисервисные сети связи, в которых ядром являются опорные IP-сети, поддерживающие частичную или полную интеграцию услуг передачи речи, данных и мультимедия.

Концепция сетей нового поколения представляет собой создание мультисервисной сети с интеграцией существующих служб с помощью использования распределенной программной коммутации. В конечном итоге, все информационные потоки интегрируются в единую сеть.

К идеологическим принципам построения NGN относят:

- доступ к сети должен осуществляться простым и удобным способом без использования промежуточных систем, но при этом применяются стандартные протоколы и сервисы в прежнем объеме;
- сеть строится на основе пакетной транспортной сети с помощью компьютерных технологий, которые способны обеспечить качество, надежность и масштабируемость, и только потом на ней будут реализованы мощные комплексы сервисов.

Возможности сетей:

- возможность создания и управления службами, которые уже существуют или будут созданы. Включает в себя службы с любыми видами кодирования и сервисами (данных, диалоговыми, одноадресными, многоадресными и т.д.), в реальном времени и вне реального времени, чувствительные к задержке и допускающие задержку;
- возможность разъединения служб и сетей с помощью разделения транспортных функций и программных служб;
- возможность взаимодействия NGN с сетями ТфОП, ЦСИС, СПС с помощью шлюзов;
- повышенное качество обслуживания (QoS) и высокий уровень безопасности.

Интернет-технология, включающая в себя IP-протоколы и технологию MPLS, является основной для мультисервисной сети. На сегодняшний день существуют несколько вариантов построения сети, которые предложены организациями ITU-T и IETF: H.323, SIP и MGCP.

Концептуальная модель информационной безопасности корпоративной сети

Для современных компаний очень важно поддержание бесперебойной работоспособности КЦ, так как это один из аспектов финансового благополучия предприятия. Чтобы обезопасить финансы компании нужно выделить основные и самые критичные компоненты сети, вывод из строя которых может привести к полной недоступности ресурсов КЦ.

Процессный подход управления качеством услуг применим и при разработке концепции обеспечения сетевой безопасности, которая опирается на четыре циклически повторяющиеся базовые составляющие: Secure (Защита), Monitor (Мониторинг), Test (Тестирование), Improve (Улучшение) [8].

Secure – проектирование и реализация технологий, направленных на обеспечение безопасности системы;

Monitor – наблюдение за процессами и технологиями безопасности, с целью оценки работоспособности и эффективности системы безопасности, обнаружения и фиксирование вторжений и нарушений правил.

Test – тестирование процессов и технологий системы на адекватность, устойчивость и предсказуемость.

Improve – интеграция новых технологий с защищаемой системой, разработка нового дизайна сети, обновление ПО и конфигураций оборудования.

Циклическая модель информационной безопасности показана на рис. 2.

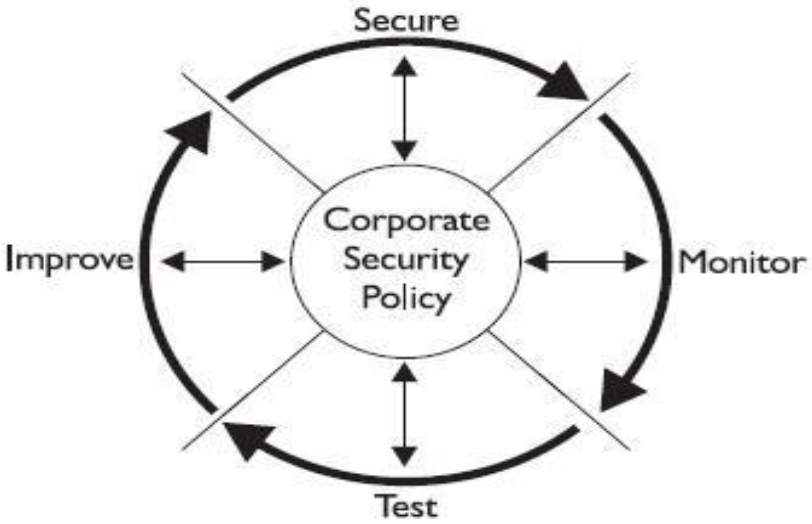

Рисунок 2

Для того чтобы построить защищенную корпоративную сеть для начала нужно разработать адекватную политику безопасности [6-9], в которой будет определяться ряд моментов, таких как:

1. План приобретений и план реализации по обеспечению информационной безопасности.
2. Разрешенные и запрещенные технологии, которые будут использоваться в системе безопасности.
3. План действий при возникновении инцидентов.
4. План, регулирующий действия и поведение рабочего персонала.
5. Перечень санкций за нарушение.
6. Составление иерархии ответственности за реализацию, поддержку, аудит, мониторинг и т.д.
7. План выбора дальнейшего развития системы безопасности.

Политика безопасности представляет собой формальное изложение правил, которому должны следовать все субъекты, получающие доступ к корпоративной сети и информации, находящейся в ней. Политика безопасности – это своего рода компромисс между безопасностью и простотой использования, безопасностью и услугами компании, ценой системы безопасности и рисками потерь.

Структура документа, характеризующая политику безопасности компании, состоит из частей – субполитик – которые описывают различные элементы системы безопасности предприятия. Субполитики могут быть представлены как: удаленный доступ, аутентификация, парольные политики, антивирусные программы и т.д.

Также немаловажным аспектом информационной безопасности компании является компетентность персонала в плане соблюдения правил, которые предусмотрены политикой безопасности. Компания, которая вкладывает в своих сотрудников финансы на дополнительное обучение и повышение их квалификации, значительно уменьшает риски возникновения внутренних угроз безопасности и повышает эффективность действий сотрудников во время сетевых атак или других внештатных ситуациях, ведь какой бы качественной и дорогостоящей не была политика безопасности, несоблюдение правил сотрудниками сделает ее бесполезной.

Объектами защиты информационной системы являются [6, 8]:

- оборудование – рабочие станции, терминалы, сервера, сетевое оборудование и т.д.;
- программное обеспечение – Операционные Системы, которые установлены на сервере или рабочей станции;
- конфиденциальная информация – данные, которые представляют коммерческую ценность для компании.

Независимо от того, сколько денег компания потратит на обеспечение безопасности, полностью защититься невозможно. Есть три основные причины, которые вызывают трудности в защите сети:

- Технологические уязвимости – модель TCP/IP, которая является основополагающей ОС, изначально разрабатывалась без учета требований безопасности. Таким образом, все ОС на данный момент имеют уязвимости, которые постоянно обнаруживаются и устраняются. Такие уязвимости несут большую угрозу ресурсам, которыми она управляет.
- Слабость политики безопасности: недостатки мониторинга, отсутствие или недостаточная проработка плана восстановления системы после сбоя, или же отсутствие политики безопасности как таковой.
- Неправильная настройка оборудования – недостаточная защищенность паролей, неправильное использование рабочих мест, установка и использование ненужных услуг и т.д.

Проектирование системы безопасности

Современная модель защиты информации представляет собой противостояние владельцев компании и злоумышленников, которые пытаются создать риски безопасности активов компании за счет создания угроз информационной безопасности (рис. 3). Владельцы компании должны предпринимать контрмеры, направленные на минимизацию рисков активов.

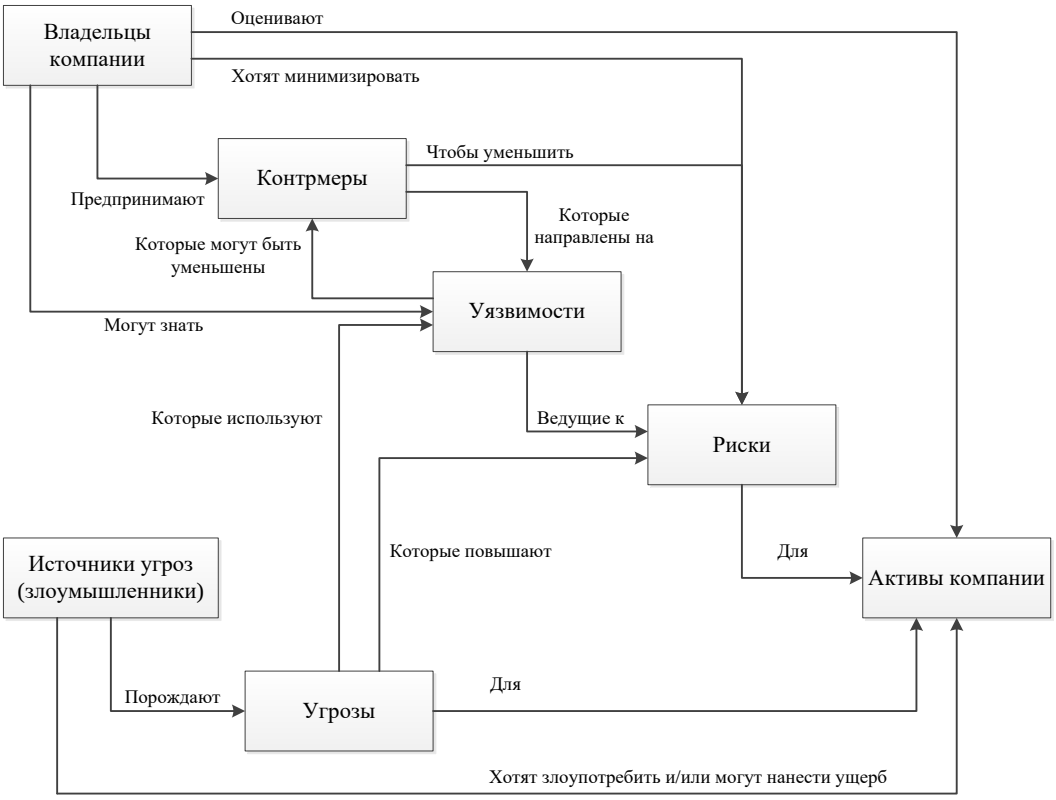

Рисунок 3

Данный подход к обеспечению защиты информации носит процессный подход, который основывается на последовательном решении таких задач, как:

1. Идентификация активов.
2. Идентификация и построение модели злоумышленника.
3. Идентификация угроз и построение модели информационной безопасности предприятия.
4. Идентификация уязвимостей активов и системы защиты компании.
5. Оценка показателя нанесения возможного ущерба владельцам активов.
6. Принятие решения о защите информации предприятия от возможных и имеющихся рисков.

В сущности, информационная безопасность ИС включает в себя две составляющие: организационную и техническую [6].

Организационная составляющая представляет собой комплекс мер, который направлен на планирование, организацию, регламентацию и документирование процессов защиты информационной безопасности.

Техническая составляющая является контрмерами в техническом обличии, которые обеспечивают информационную безопасность в виде специального оборудования и различных средств защиты.

Моделирование программно-технических мер организационной составляющей информационной безопасности контакт-центра

Одной из основных проблем безопасности информационной системы является несанкционированный доступ (НСД), который с помощью использования штатных или программных аппаратных средств приводит к нарушению установленных прав разграничения доступа пользователей или процессов к информационным ресурсам.

Примерами НСД являются:

1. Перехват паролей – выполняемый с помощью специально разработанного программного обеспечения.
2. Реализация угрозы вида «маскарад» – под данной угрозой подразумевается выполнение всех возможных действий под видом сотрудника данной компании.
3. Незаконное использование привилегий – присвоение злоумышленником прав законного представителя компании.

Во время внедрения в ИС политики безопасности авангардом защиты конфиденциальной информации от НСД являются методы аутентификации.

Для того чтобы воспользоваться функциями или данными корпоративной сети при входе в систему пользователь обязан предоставить информацию, которая позволит определить системе безопасности законность входа данного пользователя. Информация, предоставляемая пользователем, проверяется, определяются полномочия пользователя (аутентификация), разрешается доступ и взаимодействие с различными объектами системы (авторизация).

Процедура проверки прав пользователя на вход в систему состоит из трех этапов: идентификация, аутентификация и авторизация. На сегодняшний день идентификатором пользователя могут являться как пароль, личный идентификационный номер, личная карточка, так и голос, отпечатки пальцев и многое другое. Таким образом, процедура идентификации и аутентификации пользователей напрямую зависит от положений политики безопасности, внедренной в предприятие.

Исходя из внедренной компанией политики безопасности для каждого пользователя внутри системы характерен свой набор доступов и разрешений, которые не позволят ему модифицировать, удалять или препятствовать доступу к какому-либо из ресурсов или файлов системы, если у него нет на это полномочий.

Объектно-ориентированный подход позволяет дать исчерпывающее описание модели доступа пользователя к корпоративной сети за счет визуального представления процессов взаимодействия пользователя и информационной системы [2, 9]. Таким образом, использование нотации UML является неотъемлемой частью при разработке и внедрении технологий информационной безопасности.

На рис. 4 представлена модель доступа сотрудника к системе, разработанная с помощью языка UML.

Процедура входа в систему состоит из нескольких этапов:

1. Проверки введенного идентификатора пользователя с помощью обращения к БД сотрудников компании.
2. Присвоение пользователю определенных привилегий, которые основаны на статусе сотрудника в компании и прописаны во внедренной политике безопасности.
3. Непосредственный вход пользователя в систему.

При вводе пользователем неверных данных он попадает под наблюдение системы безопасности, которая в свою очередь логирует все неудачные попытки входа. В зависимости от политики безопасности количество попыток на ввод пароля будет различаться, но результат остается неизменным. При многократном вводе неверных данных пользователь становится потенциально опасным субъектом, которого система временно блокирует и оповещает службу безопасности о попытках несанкционированного доступа к системе.

Если предоставленные данные пользователем являются верными, то процедура аутентификации продолжается и пользователю присваиваются определенные привилегии, которые зависят от должности, занимаемой в компании.

Немаловажным аспектом является проверка состояния учетной записи пользователя, который пытается получить доступ к системе. Так как большинство компаний имеют деловые отношения со сторонними организациями, которые могут участвовать в разработке и

продвижении продуктов компании заказчика, нередким бывает предоставление доступа к информационной системе работникам партнерской организации. Данный вид доступа осуществляется только при согласовании со службой безопасности и предоставлении адекватного обоснования для доступа стороннего пользователя к внутренней сети предприятия. Проверка ограничений учетной записи проводится для того, чтобы узнать, активна учетная запись или нет. Если учетная запись неактивна, то пользователь сможет получить доступ только с продления учетной записи со стороны ответственных инженеров.

Рисунок 4

Алгоритм изменения файла сотрудником с учетом мер по обеспечению информационной безопасности представлен на рис. 5.

Данная модель описана с помощью сценария «как должно быть», и показывает обеспечение безопасности для угрозы «Несанкционированного изменения данных».

Модель состоит из трех контуров обеспечения безопасности:

1. Проверка прав пользователя на осуществление каких-либо действий, которая основана на политике привилегий.
2. Проверка критичности изменений данных, для оценки которой используется классификатор операций.
3. Логирование изменений (регистрация действий пользователя над объектом в таблицах логов).

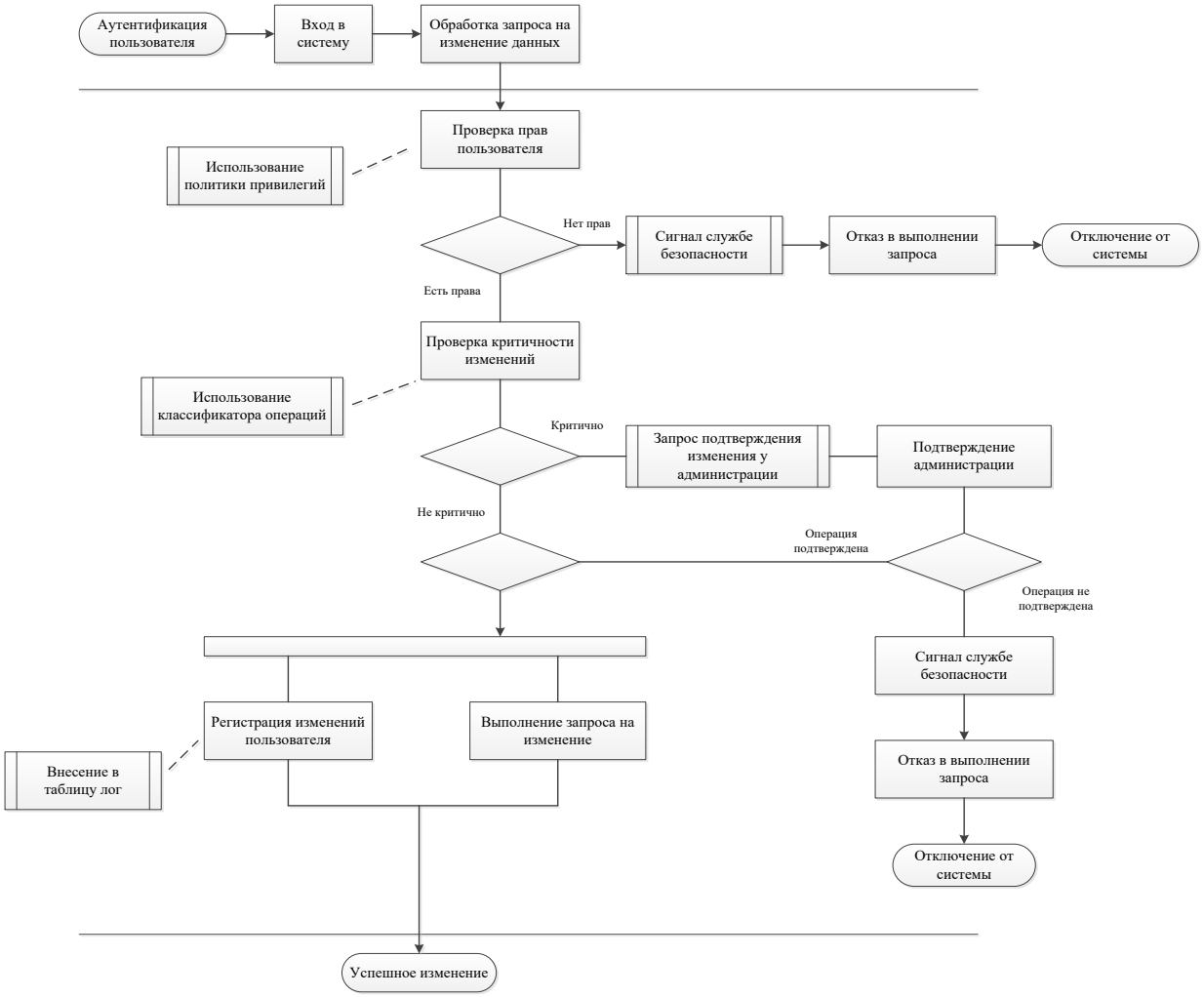

Рисунок 5

Данная модель помогает сформулировать функциональные требования к информационной безопасности системы и снизить риски несанкционированного доступа к ресурсам компании за счет:

- использования политики доступа пользователей, основанной на привилегиях;
- наличия классификатора критичности операций;
- наличия таблиц логирования операций;
- использования программно-аппаратного комплекса для подтверждения операций изменения третьим лицом;
- использование программно-аппаратного комплекса для оповещения службы безопасности в случае несоответствия привилегий или действий пользователя внедренной политике безопасности.

Моделирование программно-технических мер технической составляющей информационной безопасности контакт-центра

Тенденция развития информационных технологий и повсеместное внедрение компьютерных систем дала повод для решения сложных задач в области обеспечения информационной безопасности.

Защита информационной безопасности представляет собой комплекс мер по соблюдению трех главных свойств информации: доступности, целостности,

конфиденциальности [6, 8]. По функциональной направленности можно выделить три вида угроз информации:

1. Угроза доступности – защищаемая информация должна быть беспрепятственно доступна легитимным пользователям.
2. Угроза целостности – защищаемая информация может изменяться только пользователями, которые имеют на это соответственные полномочия, должна быть внутренне непротиворечива и должна отражать реальное положение вещей.
3. Угроза конфиденциальности – доступ к защищаемой информации могут получить только легитимные пользователи.

Угроза – это возможность потери в результате наступления определенных событий, вызванных случайно или от чьих-то преднамеренных действий.

Общую модель угроз активов ИС мультимедийного КЦ можно представить с помощью диаграммы прецедентов [3, 4] (см. рис. 6). Данная диаграмма описывает варианты реализации угроз по активам компании.

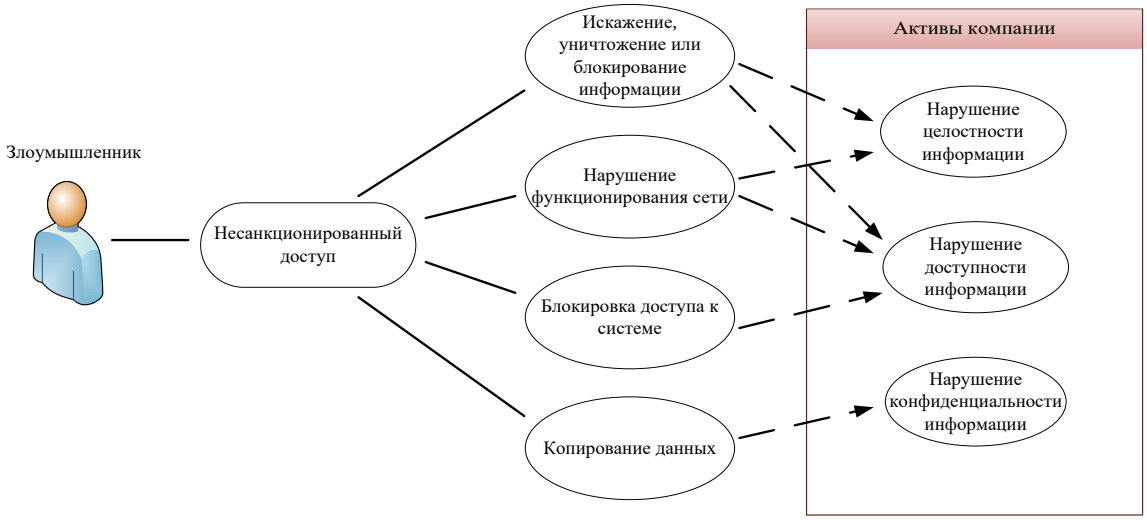

Рисунок 6

В случае с ИС мультимедийного КЦ активами компании являются полоса пропускания и серверное оборудование (см. рис. 7).

Рисунок 7

Для КЦ полоса пропускания играет одну из важнейших ролей, ведь от полосы пропускания будет зависеть как скорость передачи данных внутри сети, так и время, которое абонент или потенциальный клиент должен будет потратить для доступа к сайту или почтовому сервису. Длительное время ожидания или невозможность «достучаться» до сайта способны сильно подорвать финансовое положения компании.

Серверное оборудование, отвечающее за доступность и хранение данных, а также, поддержание работоспособности услуг и сервисов КЦ, требует высокого уровня защищенности и квалифицированного обслуживания. В современных реалиях простой оборудования является неприемлемым для бизнеса компании. Именно поэтому на сегодняшний день тенденции развития информационной и сетевой безопасностей уделяют большое внимание уменьшению времени простоя оборудования.

Сетевая атака – это пагубное воздействие на удаленный информационный ресурс с целью захватить доступ над системой, получить конфиденциальную информацию или привести атакуемый ресурс к отказу в обслуживании.

Одной из самых распространенных сетевых угроз информационной безопасности предприятия являются атаки типа DoS/DDoS-. Их популярность обусловлена тем, что являясь довольно простыми в реализации, они способны нанести огромный ущерб финансовому состоянию предприятия. Против атак данного вида труднее всего создать гарантированную защиту

DoS (от англ. Denial of Service – отказ в обслуживании) – хакерская атака, направленная на вычислительную систему с целью помешать легитимным пользователям воспользоваться атакуемым ресурсом за счет забивания полосы пропускания нелигитимным трафиком или вывода ресурса из строя. Отказ атакуемого ресурса может привести к овладению злоумышленником системой, если в нештатной ситуации ПО ресурса выдает критическую для безопасности информацию, такую как: версию ПО, часть программного кода и т.д. Чаще всего атаки данного типа направлены на дестабилизацию финансового положения атакуемой компании за счет простоя службы, которая приносит доход и принятию мер для ухода от атаки, что существенно сказывается на финансах предприятия. В настоящее время DoS/DDoS-атаки наиболее популярны среди сетевых атак, так как позволяют вывести из строя практически любую систему, при этом не оставляя юридически значимых улик.

Если DoS-атака реализовывается одновременно с большого числа компьютеров, то такая атака называется DDoS (от англ. Distributed Denial of Service – распределенная атака типа «отказ в обслуживании»).

Для того чтобы обнаружить атаку типа «отказ в обслуживании», нужно классифицировать их, знать принципы работы и правильно определить объект, на который направлена атака.

Можно выделить четыре типа DDoS атак, которые соответствуют четырем уровням модели OSI:

1. Атаки канального уровня (Layer 2) – данный вид атак направлен на исчерпание емкости сетевого канала за счет забивания полосы пропускания аномально большим количеством трафика. Вследствие чего ресурс теряет доступ к внешней сети. Во время атаки трафик измеряется в Гб/сек и его приходится обрабатывать на стороне провайдера, дата-центра.
2. Атаки сетевого уровня (Layer 3) – данный вид атак направлен на нарушение работы элементов сетевой инфраструктуры предприятия. Если у предприятия нет своей автономной системы, то борьба с этим типом атаки ведется провайдером или дата-центром.
3. Атаки транспортного уровня (Layer 4) – атаки данного типа направлена на эксплуатацию уязвимых мест TCP стека. Так как в TCP протоколе используется

таблица открытых соединений данная атака направлена именно на нее. Для борьбы с такими атаками необходим постоянный анализ поведения TCP-стека.

4. Атаки прикладного уровня (Layer 7) – данный вид атак направлен на нарушение работы Web-составляющей предприятия за счет воздействия на ресурсы сервера. Для борьбы с данным типом атаки необходим постоянный мониторинг ресурсов сервера, оптимальная параметров сервера под решаемые им задачи. Полностью защититься от атак данного вида практически невозможно.

В качестве программно-технических мер защиты от сетевых атак типа DDoS атак используют пакетные фильтры и специальное программное обеспечение

Под конкретный тип сетевых атак необходимо осуществлять настройку и управление правилами пакетной фильтрации.

Пошаговый алгоритм исследования состоит из нескольких этапов:

1. Наблюдение за характеристиками сервера и сетевым трафиком для обнаружения отклонений от статистической нормы.
2. Анализ трафика на момент присутствия сетевой атаки.
3. Настройка сервера под конкретную атаку и внесение правил фильтрации сетевого трафика.

Во время проведения исследования для каждого из типов атак необходимо использовать специальное программное обеспечение и скрипты:

- для атак HTTP flood: goldeneye;
- для «медленных» атак: sockstress, slowhttptest;
- для атак UDP flood: hping3;
- для атак SYN flood и атак на TCP-стек: hping3;
- для атак ICMP flood: hping3.

В ходе исследования необходимо провести атаки типа «отказ в обслуживании» видов: HTTP flood, «медленные» атаки, SYN flood, ICMP flood, land атаки, атаки с использованием SSL, amplification атаки. Нужно отследить аномалии в распределении ресурсов сервера и аномалии сетевого трафика для подтверждения присутствия DDoS-атаки. Непосредственно с помощью настройки сервера, добавления правил для межсетевого экранирования и пакетной фильтрации по сигнатурам защитить сервер и предотвратить возможность вывода сервера из строя. Только столкнувшись с проблемой лицом к лицу можно адекватно оценить масштаб трагедии и сориентироваться в дальнейших действиях по нейтрализации угрозы. Целью данного исследования являлась разработка эффективного метода борьбы с атаками типа «отказ в обслуживании» на основе пакетного фильтра.

В нашем исследовании в качестве пакетного фильтра был использован межсетевой экран (МЭ) Netfilter, который является стандартным для операционных систем семейства Linux. С помощью утилиты командной строки Iptables можно осуществлять настройку и управление правилами пакетной фильтрации и перенаправлением пакетов МЭ Netfilter. Из-за своей простоты и гибкости настройки выбранный МЭ снискал большую популярность среди системных администраторов, как метод борьбы с атаками типа «отказ в обслуживании». Все входящие пакеты пропускаются через цепочки правил, содержащих определенные критерии. Во время прохождения пакетом цепочки система по очереди проверяет – каким критериям соответствует данный пакет и стоит ли его пропускать дальше, удалить, передать для дальнейшего анализа или вернуть на предыдущий этап для более тщательной проверки.

Литература

1. Максименко В.Н., Филиппов А.А. Центр обработки данных в структуре системы управления качеством оператора сотовой связи // Телекоммуникации и транспорт, 2008. – № 6. – С. 47-51.
2. Гома Х. UML. Проектирование систем реального времени, параллельных и распределенных приложений: Пер. с англ., – М.: ДМК Пресс, 2011, – 704 с.
3. Максименко В.Н., Васильев М.А. Методика системного проектирования инфокоммуникационных услуг сетей 3G // Электросвязь, 2011. – № 6. – С. 38-41.
4. Артамонова Я.С., Максименко В.Н. Аналитическое моделирование ИК-услуг сетей NGN // Инновации и инвестиции, 2015. – № 6. – С. 136-142.
5. Максименко В.Н., Даричева А.Н. Методические подходы к оценке качества услуг контакт-центра // Экономика и качество систем связи, 2017. – № 1 (3). – С. 79-88.
6. Максименко В.Н., Модель угроз и методы защиты информации аутсорсингового контакт-центра виртуального оператора сотовой подвижной связи // Информационное противодействие угрозам терроризма, 2009. – № 13. – С. 92-97.
7. Максименко В.Н. Особенности оценки качества инфокоммуникационных услуг контакт-центра // T-Comm: Телекоммуникации и транспорт, 2010. – Т. 4. – № 10. – С. 39-41.
8. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи, М.: Горячая линия-Телеком, 2007, – 360 с.
9. Леоненков А.В. Объектно-ориентированный анализ и проектирование с использованием UML и IBM RATIONAL ROSE: Учебное пособие / А.В. Леоненков. – М.: Интернет Университет Информационных Технологий; БИНОМ Лаборатория знаний, 2010. – 320с.:ил.